

ASIAGAP GUIDELINES ON ICT USE IN AUDIT PROCESS

Ver.1



Issued: October 1, 2020
Effective: November 1, 2020

Contents

Objective

1. Definition of Terms	1
2. Scope of Application	1
2.1 Scope of Application	1
2.2 Onsite Audit	1
2.3 Application to Confirmation on the result of Corrective Action Requests	2
3. Competence of Auditors	2
3.1 Training of Auditors and Staff	2
3.2 Competence of Auditors and Staff	2
4. Audit Timing, Audit Time, and Audit Period	2
4.1 Audit Timing	2
4.2 Audit Time	2
4.3 Audit Period	2
5. Security	3
5.1 Ensuring Security	3
5.2 Agreement on Security	3
6. Implementation Procedure	3
6.1 Audit Application	3
6.2 Materials to be Submitted	3
6.3 Confirmation of Documentation and Specification of Matters to be Audited Carefully	3
6.4 Connectivity Test	3
6.5 Determination of Possibility of Remote Audit	3
6.6 Formulation of Audit Plan	4
6.7 Implementation of Remote Audit	4
6.7.1 Environment	4
6.7.2 Implementation of Audit	4
6.8 Implementation of Onsite Audit	4
7. Post-audit Activities	4
8. Registration	4

Objective

This document sets out guidelines for implementing some audits for the ASIAGAP certification program operated by Japan GAP Foundation (hereinafter "JGF") by means of remote audit pursuant to ASIAGAP General Regulations and GFSI Benchmarking Requirements Ver.2020.1, IAF MD 4:2018 IAF Mandatory Document for the Use of Information and Communication Technology (ICT) for Auditing/Assessment Purposes.

1. Definition of Terms

(1) ICT (Information Communication Technology)

ICT is the use of technology for gathering, storing, retrieving, processing, analyzing and transmitting information. It includes software and hardware such as smartphones, handheld devices, laptop computers, desktop computers, drones, video cameras, wearable technology, artificial intelligence, and others. (Source: IAF MD 4:2018)

(2) Remote audit

A remote audit is the method of conducting an audit of a farm remotely using ICT equipment. A remote audit must be conducted using technology such as a web conferencing system to ensure that the certifying body and the farm clearly understand each other's reactions, in other words, in an environment that allows each participant to share live audio and video instantly and indicate its intentions in an appropriate and timely manner.

(3) Onsite audit

An onsite audit is the method of conducting an audit via face-to-face meetings between the auditor, the audited farm and/or the group administration. An onsite audit is conducted in the audited fields and facilities.

2. Scope of Application

2.1 Scope of Application

These Guidelines apply to all ASIAGAP audits. Remote activities can only account for less than 50% of the audit time.

2.2 Onsite Audit

The certification body shall determine the scope of the onsite audit and the remote audit based on documents and records relating to the farm and the group administration audit, onsite conditions and other relevant factors. An onsite audit shall be required in relation to the following:

- (i) Confirmation that an HACCP-based food safety management system is incorporated in all business processes
- (ii) Matters identified in a remote audit as requiring onsite confirmation
- (iii) Other matters identified as requiring onsite confirmation

2.3 Application to Confirmation on the result of Corretive Action Requests(CARs).

The result of CARs can be confirmed remotely. If they are confirmed remotely, these Guidelines must be followed.

3. Competence of Auditors

3.1 Training of Auditors and Staff

ICT technicians can be used as staff to conduct remote audits. The certification body must provide officers with necessary training covering the aspects shown below and must clearly document requirements in relation to ISO/IEC17065 and IAF MD 4 and make these requirements known to auditors and staff.

- (i) Information security
- (ii) How to operate ICT equipment
- (iii) Remote audit procedures, methods and their potential impact on the audit results

3.2 Competence of Auditors and Staff

The certification body shall document procedures for assessing auditor and staff competence described below in relation to conducting a remote audit and determine the possibility of remote audit implementation ((iv) refers to competence of auditors only). The competence of an auditor to conduct a remote audit shall be assessed in a witness audit prior to any remote audit. A witness audit must be conducted for an audit which involves a remote audit and the witnessing of the onsite audit elements of this audit must be done onsite.

- (i) Ability to use the ICT equipment used in a remote audit
- (ii) Completion of sufficient training to conduct a remote audit, ability to competently conduct a remote audit, and understanding of risks relating to the accuracy of information gathered in a remote audit
- (iii) Understanding of security risks involved in a remote audit
- (iv) Understanding of potential risk impact of a remote audit on audit results and competence to conduct a remote audit accurately

4. Audit Timing, Audit Time, and Audit Period

4.1 Audit Timing

Requirements in relation to audit timing shall be in accordance with the General Regulations.

4.2 Audit Time

Audit time shall be the sum total of the remote audit time and onsite audit time. If audit time is shorter than usual (than an audit done entirely onsite), the certification body must justify why the audit time was shorter.

4.3 Audit Period

A remote audit must be conducted before an onsite audit and both audits must be completed

within thirty (30) days.

If the onsite audit cannot be completed within thirty (30) days after the remote audit due to the risk of infection, disaster or other cause, the period for completion of the onsite audit may be extended to a maximum of ninety (90) days. If an audit cannot be completed within thirty (30) days, the reason for extension and a risk assessment for the audit extension must be submitted to JGAP Foundation ("JGF") and approval from JGF must be obtained.

5. Security

5.1 Ensuring Security

The certification body shall be sure to implement measures to keep information confidential throughout the entire audit including the planning, reporting and follow-up stages.

5.2 Agreement on Security

Prior to the audit, the certification body and the farm shall agree on security, as well as measures to protect information and mutual understanding where responsibility lies, relating to audits such as data, voice recordings, screen shots etc.

If using the video or sound recording functions of remote audit tools, the certification body and the farm shall agree on the scope and purpose of such use and the timing of the disposal of such recordings.

The agreement on security shall be made in writing and the agreement document shall be retained. If there is no written agreement on security, a remote audit cannot be conducted.

6. Implementation Procedure

6.1 Audit Application

The remote audit application form shall include the details shown below.

- (1) Equipment, platform and resources to be used in the remote audit
- (2) Participants in audit
- (3) Use of ICT such as cloud platform for GAP-related reports and other materials

6.2 Materials to be Submitted

The farm shall submit the materials shown below to the certification body.

- (1) List of fields and facilities
- (2) Maps of fields and facilities
- (3) Results of risk assessments of harvesting processes and produce handling processes
- (4) Internal audit results and results of improvement of non-conforming items identified in internal audit

6.3 Confirmation of Documentation and Specification of Matters to be Audited Carefully

The certification body shall confirm the submitted documentation.

The certification body shall identify the potential impact of the audit results of previously audited farms and previously submitted materials on the remote audit and the risks involved in using ICT to gain an understanding and make a record of matters to be audited carefully (including matters to be audited on site).

6.4 Connectivity Test

The connectivity test, remote audit and onsite audit shall be conducted by the same auditor.

Confirmation of the communication environment and video and image accuracy as part of paper-based document and onsite confirmation shall be required.

6.5 Determination of Possibility of Remote Audit

The certification body shall conduct a remote audit risk assessment from the perspectives described below, including information about the remote audit obtained in 6.1 Audit application form, 6.2 Materials to be submitted and 6.4 Connectivity test and determine the possibility of remote audit implementation. It shall conduct an interview survey where necessary as part of the risk assessment. The certification body shall record remote audit risk assessment results and whether remote audit implementation is possible.

- (1) Corrective action requests made in the immediately preceding audit
- (2) ICT equipment and communication environment (communication speed, noise) to be used
- (3) Competence of the auditor in charge and competence of the audited farm in regard to use of the foregoing
- (4) Ensuring of information security and confidentiality

6.6 Formulation of Audit Plan

An audit plan shall be formulated specifying how ICT will be used in the remote audit and the onsite audit. The audit plan shall reflect the results of identification of matters to be audited carefully identified in 6.3.

6.7 Implementation of Remote Audit

6.7.1 Environment

A quiet location where audio and video can be easily shared shall be selected.

6.7.2 Implementation of Audit

Audit proceedings (includes the start, the closing meeting and the report of audit results) shall be in accordance with the General Regulations and the audit shall be implemented in accordance with the set plan as far as possible.

The audit start time and finish time and audit participants shall be recorded in the audit report. Any technical issues shall also be recorded in the report.

6.8 Implementation of Onsite Audit

The onsite audit shall be conducted in accordance with the audit plan. An onsite audit shall also be conducted with respect to matters judged in the remote audit as requiring onsite

confirmation.

7. Post-audit Activities

After an audit decision has been made, the auditor shall destroy records obtained through use of the video or sound recording functions of remote audit tools.

8. Registration

The certification body shall report certification information to JGF, specifying that a remote audit took place, and JGF shall record the certified farm/group, specifying that a remote audit took place.

End



Japan GAP Foundation

3-29 Kioicho, Chiyoda-ku, Tokyo, Japan
Floor 4, Nippon Nogyo Kenkyusho Bldg.

URL: <http://jgap.jp>